CLAIMS

1. A method for securing ownership for a two-part device with a physical unit and a virtual unit, wherein ownership of the two-part device is efficiently initiated, maintained, and transferred, comprising the steps of:

initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure; and

utilizing a double safety mechanism to activate ownership services via the virtual unit for the physical unit.

2. The method of claim 1 wherein the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, an e-Services Host, a Control Console, and a Secure Data Storage Unit.

3. The method of claim 2 wherein the Control Console is a web browser.

4. The method of claim 2 wherein the Secure Data Storage Unit is a memory controllable by the user.

5. The method of claim 2 wherein the Secure Data Storage Unit is a physical device under control of the user.

6. The method of claim 2 wherein the Secure Data Storage Unit is a virtual device under control of the user.

7. The method of claim 1 wherein the double safety mechanism includes the steps of:

upon the virtual unit upon being activated, generating a first Knowledge Element and a first Proof of Knowledge Check Element;
storing the first Knowledge Element in a Secure Storage Unit and sending the Proof of Knowledge Check Element to the virtual unit;
upon the virtual unit receiving the Proof of Knowledge Check Element, storing, by the virtual unit the first Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store and generating, by the virtual unit, a second Knowledge Element and a second Proof of Knowledge Check Element;
storing, by the virtual unit, the second Knowledge Element in an Ownership Knowledge Element Storage Unit;
sending, by the virtual unit, the second Proof of Knowledge Check Element to the physical unit; and
storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit.

8. The method of claim 7 wherein generating the first Knowledge Element and the first Proof of Knowledge Check Element is accomplished by the physical unit.

9. The method of claim 7 wherein generating the first Knowledge Element and the first Proof of Knowledge Check Element is accomplished by a Control Console coupled to the virtual unit, the physical unit and to a Secure Data Storage Unit.

10. The method of claim 7 wherein storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit is accomplished by the physical unit by storing in a memory of the physical unit.

11. The method of claim 7 wherein storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit is accomplished by a Control Console by storing in a Secure Data Storage unit.

12. The method of claim 1 wherein initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure includes utilizing an Internet address recorded in the physical unit to send the activation signal.

13. The method of claim 1 wherein initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure includes utilizing a uniform resource identifier recorded in the physical unit to send the activation signal to the virtual unit.

14. A method for taking ownership of a part-physical, part-virtual device, comprising the steps of:

communicating, by a physical unit of the device, by sending an activation signal to a virtual unit of the device; and

registering ownership of the device using a double knowledge check-proof of knowledge check mechanism.

15. The method of claim 14 wherein the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, an e-Services Host, a Control Console, and a Secure Data Storage Unit.

16. The method of claim 15 wherein the Control Console is a web browser.

17. The method of claim 15 wherein the Secure Data Storage Unit is a memory controllable by the user.

18. The method of claim 15 wherein the Secure Data Storage Unit is a physical device under control of the user.

19. The method of claim 15 wherein the Secure Data Storage Unit is a virtual device under control of the user.

20. The method of claim 14 wherein the double knowledge check-proof of knowledge check mechanism includes the steps of:

upon the virtual unit upon being activated, generating a first Knowledge Element and a first Proof of Knowledge Check Element;

storing the first Knowledge Element in a Secure Storage Unit and sending the Proof of Knowledge Check Element to the virtual unit;

upon the virtual unit receiving the Proof of Knowledge Check Element, storing, by the virtual unit the first Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store and generating, by the virtual unit, a second Knowledge Element and a second Proof of Knowledge Check Element;

storing, by the virtual unit, the second Knowledge Element in an Ownership Knowledge Element Storage Unit;

sending, by the virtual unit, the second Proof of Knowledge Check Element to the physical unit; and

storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit.

21. The method of claim 20 wherein generating the first Knowledge Element and the first Proof of Knowledge Check Element is accomplished by the physical unit.

22. The method of claim 20 wherein generating the first Knowledge Element and the first Proof of Knowledge Check Element is accomplished by a Control Console coupled to the virtual unit, the physical unit and to a Secure Data Storage Unit.

23. The method of claim 20 wherein storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit is accomplished by the physical unit by storing in a memory of the physical unit.

24. The method of claim 20 wherein storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit is accomplished by a Control Console by storing in a Secure Data Storage unit.

25. The method of claim 14 wherein activating, by a user, an ownership trigger of a physical unit of the device includes using an Internet address recorded in the physical unit to send the activation signal.

26. The method of claim 14 wherein activating, by a user, an ownership trigger of a physical unit of the device includes utilizing a uniform resource identifier recorded in the physical unit to send the activation signal to the virtual unit.

27. A two-part device with a physical unit and a virtual unit, wherein ownership of the two-part device is efficiently initiated, maintained, and transferred, comprising:

a physical unit, having an ownership activation trigger for initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure; and

the virtual unit, which communicates with the physical unit upon activation;

wherein the physical unit and the virtual unit employ a double safety mechanism to register ownership services.

28. The device of claim 27 wherein the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, an e-Services Host, a Control Console, and a Secure Data Storage Unit.

29. The device of claim 28 wherein the Control Console is a web browser.

30. The device of claim 28 wherein the Secure Data Storage Unit is a memory controllable by the user.

31. The device of claim 28 wherein the Secure Data Storage Unit is a physical device under control of the user.

32. The device of claim 28 wherein the Secure Data Storage Unit is a virtual device under control of the user.

33. The device of claim 27 wherein the virtual unit is activated and in the double safety mechanism, a first processor in the physical unit generates a first Knowledge Element and a first Proof of Knowledge Check Element, stores the first Knowledge Element in a Secure Storage Unit and sends the Proof of Knowledge Check Element to the virtual unit, which authenticates and stores the

Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store and a second processor in the virtual unit generates a second Knowledge Element and a second Proof of Knowledge Check Element, wherein the second Proof of Knowledge Check Element is stored in an Ownership Knowledge Element Storage Unit; and the virtual unit sends the second Proof of Knowledge Check Element to the physical unit, which authenticates and stores the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit.

34. The device of claim 33 wherein the physical unit generates the first Knowledge Element and the first Proof of Knowledge Check Element.

35. The device of claim 33 further including a Control Console coupled to the virtual unit, the physical unit and to the Secure Data Storage Unit, wherein the Control Console generates the first Knowledge Element and the first Proof of Knowledge Check Element.

36. The device of claim 33 wherein the physical unit stores the second Proof of Knowledge Check Element in the second Proof of Knowledge Check Store unit that is a memory of the physical unit.

36. The device of claim 33 further including a Control Console coupled to the virtual unit, the physical unit and to a Secure Data Storage Unit, wherein the Control Console stores the second Proof of Knowledge Check Element in the Ownership Knowledge Element Storage Unit.

37. The device of claim 27 wherein the ownership activation trigger utilizes an Internet address recorded in the physical unit to send the activation signal.

38. The device of claim 27 wherein the ownership activation trigger utilizes a uniform resource identifier recorded in the physical unit to send the activation signal to the virtual unit.

39. A system for taking ownership of a part-physical, part-virtual device, comprising:

an activation trigger, located on a physical unit of the device, for initiating an activation signal; and

the physical unit of the system, coupled to the activation trigger, for sending the activation signal to a virtual unit of the system; and

the virtual unit of the system, arranged to communicate with the physical unit of the system, for registering ownership of the device using a double knowledge check-proof of knowledge check mechanism.

40. The system of claim 39 wherein the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, an e-Services Host, a Control Console, and a Secure Data Storage Unit.

41. The system of claim 40 wherein the Control Console is a web browser.

42. The system of claim 40 wherein the Secure Data Storage Unit is a memory controllable by the user.

43. The system of claim 40 wherein the Secure Data Storage Unit is a physical device under control of the user.

44. The system of claim 40 wherein the Secure Data Storage Unit is a virtual device under control of the user.

45. The system of claim 39 wherein the double knowledge check-proof of knowledge check mechanism is a mechanism wherein the virtual unit validates the identity of the physical unit using a proof of knowledge check that corresponds to a knowledge element of the physical unit and the physical unit validates the identity of the virtual unit using a proof of knowledge check that corresponds to a knowledge element of the virtual unit.

46. The system of claim 39 wherein ownership is registered when the physical unit communicates with the virtual unit via an Internet address associated with the virtual unit.

47. The system of claim 46 wherein the virtual unit includes a first storage location for an Ownership Knowledge Element Store, coupled to store a knowledge element for the virtual unit, a second storage location for an Ownership Proof of Knowledge Check Store, coupled to receive an Ownership Proof of Knowledge Check from the physical unit, and an Ownership State Machine, coupled to the Ownership Knowledge Element Store and the Ownership Proof of Knowledge Check Store, for beginning in a Not Yet Activated state, transitioning to an Activated state upon successful completion of the double knowledge check-proof of knowledge check mechanism, and transitioning to an Owned state when ownership has been established.

48. The system of claim 47 further including a console, coupled to the virtual unit via a network connection and to a Secure Storage Unit, for maintaining a Knowledge Element Store and a Proof of Knowledge Check Store in the Secure Storage Unit and, upon

user selection, for generating a first Knowledge Element and a corresponding first Proof of Knowledge Check for the part-physical, part-virtual device, storing the first Knowledge Element in the Secure Storage Unit and sending the first Proof of Knowledge Check to the virtual unit.

49. The system of claim 48 wherein the virtual unit, upon receiving the first Proof of Knowledge Check, stores the first Proof of Knowledge Check in the Ownership Proof of Knowledge Check Store and generates a second Knowledge Element and a corresponding second Proof of Knowledge Check, stores the second Knowledge Element in the Ownership Knowledge Element Store and sends the corresponding second Proof of Knowledge Check to the console, which stores the corresponding second Proof of Knowledge Check in the Secure Storage, whereupon the virtual unit advances the Ownership State Machine to an Owned state.

50. The system of claim 49 wherein the Owned state allows a full range of predetermined owner services to be accessed using the double knowledge check-proof of knowledge check mechanism.

51. The system of claim 50 wherein the Owned state allows a full range of predetermined owner services to be transferred using the double knowledge check-proof of knowledge check mechanism.